(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 801 995**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **99 15437**

(51) Int Cl[7] : **G 06 F 17/60**, H 04 L 9/32, H 04 Q 7/20

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 07.12.99.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 08.06.01 Bulletin 01/23.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *DUVAL BRUNO* — FR.

(72) **Inventeur(s) :** DUVAL BRUNO.

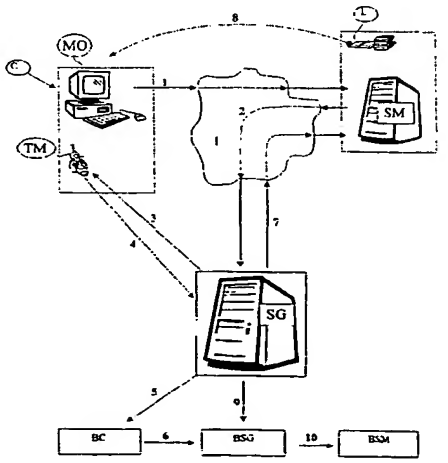
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** PONTET ET ALLANO SARL.

(54) PROCEDE ET SYSTEME DE GESTION D'UNE TRANSACTION SECURISEE A TRAVERS UN RESEAU DE COMMUNICATION.

(57) L'invention concerne un procédé de gestion d'une transaction sécurisée à travers un réseau de communication (I), par exemple de type Internet, dans lequel un client (C), lors de la commande d'un produit (L) sur un site marchand (SM), transmet (1) son numéro d'identifiant vers le site marchand à travers le réseau de communication. Selon l'invention, le site marchand transmet (2) ensuite les références du produit, l'identifiant du client et l'identifiant dudit site marchand vers un serveur de gestion (SG). Puis le serveur de gestion (SG) contacte (3) le client (C) en envoyant un message sur le téléphone mobile (TM) dudit client afin d'obtenir (4) l'accord du client et une authentification dudit client. Enfin, le serveur de gestion (SG) confirme (7) l'accord du client au site marchand (SM) qui délivre (8) le produit commandé (L) au client (C).

Utilisation pour le commerce électronique.



FR 2 801 995 - A1

Procédé et système de gestion d'une transaction sécurisée à travers un réseau de communication.

L'invention concerne un procédé de gestion d'une transaction sécurisée à travers un réseau de communication, par exemple de type Internet, dans lequel un client, lors de la commande d'un produit sur un site marchand, transmet son numéro d'identifiant, différent du numéro de carte de crédit, vers le site marchand à travers le réseau de communication. Elle vise également un système de gestion de transaction mettant en œuvre ledit procédé.

Le réseau de communication de type Internet est un réseau non sécurisé dans lequel les informations transitant d'un point à un autre peuvent être interceptées. Cet état de fait est un obstacle à l'évolution du commerce électronique. En effet, les acheteurs hésitent à donner leur numéro de carte de crédit à des sites marchands à travers l'Internet. D'une autre part, les sites marchands et les banques font face à de nombreuses plaintes pour cartes de crédits volées ou achat non confirmé, l'acheteur refusant l'achat en affirmant n'avoir pas confirmé son achat. Ainsi les sites marchands ne font pas confiance aux acheteurs et tardent à livrer les produits aux acheteurs, et les banques conservent l'argent des transactions le plus longtemps possible avant de créditer les sites marchands.

On connaît des systèmes qui, pour améliorer la sécurité, se basent sur la téléphonie mobile car celle-ci présente l'intérêt d'être nominative. Ainsi il existe déjà un système de transaction sécurisée basé sur une infrastructure à clé publique mettant en œuvre notamment l'algorithme RSA. Ce système implique un opérateur ainsi qu'une technologie de chiffrement à base de tiers de confiance.

Par ailleurs, un opérateur de communication mobile a développé un système de paiement sécurisé dans lequel le site

marchand envoie directement un message selon la norme SMS (« Short Message Service » en langue anglaise) sur le téléphone mobile de l'acheteur. Le téléphone mobile de l'acheteur comporte un double lecteur pour une carte SIM (« Subscriber Identity Module », en langue anglaise) et une carte bancaire, et permet d'envoyer une demande d'autorisation directement à la banque de l'acheteur. Un tel système ne pourrait actuellement être déployé à grande échelle puisqu'il est lié à un opérateur unique et qu'il implique l'utilisation de téléphones mobiles adaptés qui ne représentent qu'une faible partie du parc actuel de téléphones mobiles.

L'invention vise à apporter une solution aux problèmes cités ci-dessus en proposant un système de transaction sécurisé qui instaure un climat de confiance entre les acheteurs et les sites marchands.

Un but de l'invention est de proposer une technologie peu onéreuse à mettre en œuvre et demandant un investissement minimum pour le client.

Un autre but de l'invention est de réaliser une technologie capable de s'intégrer dans tout type de téléphone mobile capable de recevoir des messages selon la norme SMS par exemple.

Pour atteindre les buts ci-dessus, l'invention propose donc un procédé de gestion d'une transaction sécurisée à travers un réseau de communication, par exemple de type Internet, dans lequel un client, lors de la commande d'un produit sur un site marchand, transmet son numéro d'identifiant vers le site marchand à travers le réseau de communication. Selon l'invention :

- le site marchand transmet ensuite les références du produit, l'identifiant du client et l'identifiant dudit site marchand vers un serveur de gestion.
- le serveur de gestion transmet un message sur le téléphone mobile dudit client afin d'obtenir l'accord du client et une authentification dudit client, puis

- le serveur de gestion confirme l'accord du client au site marchand qui délivre le produit commandé au client.

Par ailleurs, le serveur de gestion conserve la trace de la transaction qui se sera déroulée de façon non répudiable.

Selon un mode de mise en œuvre de l'invention, l'authentification met en œuvre une table d'identification du client stockée dans un moyen de stockage du téléphone mobile dudit client ainsi que dans le serveur de gestion. Par ailleurs, le serveur de gestion possède une base de données capable de gérer une multitude de tables d'une multitude de clients.

Pour effectuer l'authentification, on peut avantageusement utiliser un procédé d'identification sécurisée ayant fait l'objet d'un brevet sous le numéro de publication FR 2 745 136. Ce document décrit un procédé d'identification sécurisée pour la communication entre un poste utilisateur et un poste serveur par l'intermédiaire d'un réseau de communication non sécurisé de type Internet. D'une manière générale, le poste utilisateur est destiné à lire le contenu d'un support d'identification tel qu'une matrice, en fonction d'informations provenant du poste serveur. Pour ce faire, on établit une liaison entre le poste serveur et le poste utilisateur, on choisit un code serveur de manière aléatoire au niveau du poste serveur, on transmet dans un premier sens serveur-utilisateur des données représentatives du code serveur, on reconnaît, à l'aide desdites données, dans le contenu du support d'identification, un code utilisateur correspondant, on transmet dans un second sens utilisateur-serveur le code utilisateur, et on valide l'identification de l'utilisateur si le code utilisateur est identique au code serveur. Ce procédé ne fait intervenir aucun tiers de confiance contrairement au système de cryptage classique de type RSA qui nécessite un tiers de confiance à qui l'on confie des clés de décryptage.

Le procédé d'identification sécurisée est utilisé ici afin de permettre au serveur de gestion d'authentifier le client.

Selon une caractéristique de l'invention, la table d'identification du client peut être stockée dans le moyen de stockage du téléphone mobile du client de manière codée de sorte que l'accès à ladite table d'identification par un logiciel de communication nécessite un code secret uniquement connu par le client et par le serveur de gestion (SG).

Le logiciel de communication stocké dans le moyen de stockage du client est un programme informatique de faible taille qui gère la communication avec le serveur de gestion.

La table d'identification du client est de préférence une table contenant des caractères alphanumériques. Chaque caractère est convenablement adressé. Dans le moyen de stockage, qui peut être une carte SIM, du téléphone mobile, la table d'identification du client peut être stockée de manière codée, c'est-à-dire avec un décalage des caractères alphanumériques de sorte que l'adressage soit faussée. Ainsi pour adresser correctement ladite table d'identification du client, le logiciel de communication nécessite le code secret.

Le code secret utilisé peut être un code à plusieurs chiffres également utilisé pour sécurisé le clavier du téléphone mobile du client.

L'homme du métier comprendra aisément que tout système permettant d'authentifier le client peut être utilisé.

Selon l'invention, à chaque authentification du client, le serveur de gestion (SG) réduit la table d'identification du client stockée dans ledit serveur de gestion (SG). En fait, après chaque authentification, le serveur de gestion effectue une mise à jour en supprimant de la table d'identification du client les caractères utilisés pour réaliser l'authentification afin d'éviter que les mêmes caractères ne soient utilisés deux fois.

Suivant une caractéristique avantageuse de l'invention, le serveur de gestion possède un ensemble de données sur le client, notamment des coordonnées bancaires nécessaires pour

débiter le compte bancaire dudit client. En fait le serveur de gestion possède une base de données « client » dans laquelle il répertorie l'ensemble des informations concernant le client. Les informations concernant le client peuvent provenir de l'opérateur de téléphonie mobile chez qui le client est affilié ou une banque partenaire, ou directement du client lors de son inscription au serveur de gestion.

Suivant une autre caractéristique avantageuse de l'invention, le serveur de gestion possède un ensemble de données sur le site marchand, notamment des coordonnées bancaires nécessaires pour alimenter le compte bancaire dudit site marchand une fois que le client a reçu le produit commandé. De la même façon que pour le client, le site marchand est référencé dans le serveur de gestion grâce à une base de données « marchand ». Le serveur de gestion peut n'accepter des sites marchands que sous certaines conditions de qualité.

Avantageusement la communication entre le serveur de gestion et le site marchand peut s'effectuer de manière chiffrée. On peut également réaliser la communication entre le serveur de gestion et le site marchand à l'aide du procédé d'identification sécurisée en ayant préalablement stockée dans le site marchand et dans le serveur de gestion une table d'identification dudit site marchand.

De préférence, le numéro d'identifiant du client est un numéro du téléphone mobile du client. Le numéro d'identifiant peut avantageusement être le numéro de téléphone mobile accompagné du pays de résidence du client. Dans une autre variante de l'invention, le numéro d'identifiant peut être un numéro de référence que le client a obtenu lors de son affiliation au service de transaction sécurisée sur un site du serveur de gestion par exemple.

Selon un mode de mise en œuvre de l'invention, le message envoyé au client par le serveur de gestion comprend les références du produit commandé, et les messages échangés entre le client et le serveur de gestion sont chiffrés. Les références du produit peuvent être le nom du produit, le prix du produit et le nom du site marchand. Le produit vendu peut

par exemple être un objet à expédier ou une information à communiquer par Internet.

La présente invention concerne également un système de gestion d'une transaction sécurisée à travers un réseau de communication, par exemple de type Internet, comprenant :

- un site marchand connecté au réseau de communication,
- un point d'accès connecté au site marchand à travers le réseau de communication, le point d'accès étant utilisé par un client désirant acheter un produit sur le site marchand,
- un serveur de gestion pour :
  - recevoir un identifiant du client par le site marchand,
  - authentifier le client en communicant avec ledit client à travers un téléphone mobile dudit client, l'authentification nécessitant notamment que le client tape un code secret sur son téléphone mobile,
  - débiter le compte bancaire du client,
  - adresser une confirmation de transaction audit site marchand une fois le client authentifié et son compte bancaire débité, et
  - recevoir une confirmation de livraison du produit chez le client afin de créditer le compte bancaire du site marchand.

Selon un mode de réalisation préféré du système, le téléphone mobile du client comporte un moyen de stockage dans lequel est stocké un logiciel de communication avec le serveur de gestion.

De préférence, le serveur de gestion est agencé pour gérer, d'une part pour chaque client, une liste des transactions effectuées sur une période donnée, et d'autre part pour chaque site marchand, une liste des commandes obtenues sur une période donnée.

D'autres avantages et caractéristiques de l'invention apparaîtront à l'examen de la description détaillée d'un mode

de mise en œuvre nullement limitatif, et des dessins annexés sur lesquels :

- la figure 1 est un schéma simplifié mettant en œuvre le procédé selon l'invention, et
- la figure 2 est un organigramme simplifié des étapes du procédé selon l'invention.

Bien que l'invention n'y soit pas limitée, on va maintenant décrire l'application du procédé selon l'invention à l'achat, par un client, d'un livre sur un site marchand à travers le réseau Internet.

On voit sur la figure 1 l'ensemble des éléments (référencés par des lettres) et des mouvements d'informations (référencés par des numéros) qui permettent essentiellement de réaliser le procédé selon l'invention. On distingue quatre catégories d'éléments. La première catégorie est le client C désireux d'acheter un livre sur le réseau Internet I. La deuxième catégorie est le site marchand SM proposant un service de vente de livres sur le réseau Internet. La troisième catégorie est le serveur de gestion SG qui gère les transactions financières entre le client et le site marchand SM. La quatrième catégorie regroupe la banque BC du client C, la banque BSG du serveur de gestion SG et la banque BSM du site marchand SM. Seul le serveur de gestion SG est en contact avec les banques BC, BSG et BSM.

Le client C possède un micro ordinateur MO avec lequel il peut se connecter sur le réseau Internet I. Le client C possède également un téléphone mobile TM muni d'une carte SIM. La carte SIM contient un programme informatique PI de faible taille qui a été stocké par l'opérateur de téléphonie mobile auquel le client est affilié lors de l'acquisition du téléphone mobile. Le programme informatique PI peut également être téléchargé via la liaison GSM sur la carte SIM lors d'une inscription par le client à un service de transaction sécurisé géré par le serveur de gestion SG selon l'invention. Le programme informatique PI est destiné à gérer la communication entre le serveur de gestion SG et une table T, contenant des caractères alphanumériques, stockée dans la carte SIM. La table T a

également été téléchargée dans la carte SIM par l'opérateur de téléphonie mobile. D'une façon générale, on peut envisager que la table T soit téléchargée dans la carte SIM via liaison GSM par l'opérateur de téléphonie mobile, par le serveur de gestion SG ou par une banque partenaire. La communication via liaison GSM est effectuée selon la norme SMS. Le serveur de gestion SG possède une copie de la table T. L'accès à la table T par le programme informatique PI nécessite un code secret. Le code secret peut être une clé permettant au programme informatique PI de décoder la table T préalablement stockée sous forme codé(par exemple un décalage de tous les caractères de trois cases vers la droite). Le code secret peut par exemple être transmis au client, par courrier ou autre moyen, lors du téléchargement de la table T codée. Cependant le client peut par la suite modifier son code secret (la table T codée est par conséquent modifiée par le programme informatique PI) de sorte que désormais seul le client connaît son nouveau code secret.

Le site marchand SM est abonné au service lié à la transaction sécurisée selon l'invention et propose dans son site de vente un moyen de paiement utilisant ledit service. Le site marchand SM contient un programme informatique simple de communication avec le serveur de gestion SG. Un programme informatique simple stocké dans le site marchand SM permet de conserver l'intelligence de la communication dans le serveur de gestion SG et d'éviter ainsi de nombreuses mises à jour.

Le serveur de gestion SG possède une base de données « client » dans laquelle est répertorié le client C ainsi que d'autres données fournies, par exemple, par l'opérateur de téléphonie mobile. Les autres données sont par exemple les coordonnées bancaires et l'adresse de résidence principale du client C. Le serveur de gestion SG possède également une base de données « marchand » dans laquelle est répertorié l'ensemble de sites marchands abonnés au service de transaction sécurisée ainsi que leurs coordonnées bancaires. Le serveur de gestion SG peut n'accorder l'abonnement qu'aux sites marchands qu'il considère fiable, ceci a pour effet d'accroître la confiance du

client vis à vis de l'achat à effectuer sur un site marchand garanti par le serveur de gestion.

On voit sur la figure 1, les différentes étapes du procédé selon l'invention, numérotées de 1 à 10 lors d'une opération d'achat. Au cours de l'étape 1, le client C se connecte au site marchand SM à travers le réseau Internet I, choisit le livre L qu'il désire acheter et transmet son numéro de téléphone mobile ainsi que son pays de résidence après avoir choisi le paiement par transaction sécurisée. Le client peut joindre, à la place du numéro de téléphone mobile et du pays de résidence, un numéro de référence obtenu au moment de son inscription directe sur un site du serveur de gestion SG ou auprès d'un opérateur de télécommunication mobile. Le site marchand SM envoie, sous forme chiffrée de manière classique, le titre du livre, le prix du livre, le numéro de téléphone du client et le pays de résidence du client au serveur de gestion SG à travers le réseau Internet I. Le serveur de gestion SG reçoit les informations transmises par le site marchand SM et vérifie, en consultant la base de données « client », que le numéro de téléphone du client et son pays de résidence correspondent bien à un client abonné au service de transaction sécurisée.

Ensuite, le serveur de gestion SG va vérifier, au cours des étapes 3 et 4, l'authenticité du client et obtenir son accord pour l'achat du livre L. Les étapes 3 et 4 mettent en œuvre le procédé d'identification sécurisée breveté sous le numéro de publication FR 2 745 136 auquel le lecteur est invité à se reporter. D'une façon générale, le serveur de gestion SG appelle le téléphone mobile TM du client C. Le téléphone mobile TM prévient le client C de l'arrivée d'un message. A l'aide de la norme SMS, le serveur de gestion SG envoie à l'étape 3 un message contenant les informations sur le livre L, le nom du site marchand SM et une phrase demandant au client C de taper son code secret s'il désire valider l'achat du livre L. Le message s'affiche sur l'écran du téléphone mobile TM du client C. Le serveur de gestion SG envoie également un défi selon la norme SMS en utilisant le procédé d'identification sécurisée.

Le défi consiste à choisir aléatoirement dans la table T stockée dans le serveur de gestion SG, un ensemble de caractères dit code serveur, à déterminer l'adresse du code serveur, puis à inclure l'adresse du code serveur dans le message de l'étape 3. L'adresse du code serveur n'est pas affichée et est prise en charge par le programme informatique PI stocké dans la carte SIM du téléphone mobile TM. Lorsque le client C valide l'achat en tapant son code secret, le programme informatique PI calcule une réponse non répudiable basée sur la table T contenue dans la carte SIM, le code secret, le défi (code serveur) envoyé par le serveur de gestion ainsi que les informations contenues dans le message SMS envoyé par le serveur de gestion. A titre d'exemple non limitatif, ledit calcul peut consister à un décalage de tous les caractères de trois cases vers la gauche. On détermine ainsi un ensemble de caractères dit code client.

Ensuite, à l'étape 4, le programme informatique PI envoie, selon la norme SMS, un message contenant le code client au serveur de gestion SG. Le serveur de gestion SG compare le code serveur et le code client. L'achat est validé lorsque le code client égale le code serveur. Puis, le serveur de gestion SG effectue une mise à jour en supprimant de la table d'identification du client stockée chez lui le code serveur, c'est-à-dire les caractères qui ont servi à l'authentification. Ainsi, l'adresse envoyée via liaison GSM n'est jamais la même pour un client donné effectuant de nombreux achats. Le fait de stocker la table d'identification du client de manière codée et de supprimer de la table d'identification du client stockée dans le serveur de gestion les caractères utilisés pour l'authentification, permet de renforcer la sécurité et de rendre inutilisable une table d'identification volée.

Ainsi lorsque le client est authentifié, le serveur de gestion peut alors à l'étape 5 contacter la banque BC du client C pour que la banque BC débite le compte du client C de la somme correspondant au livre L et crédite à l'étape 6 le compte bancaire du serveur de gestion SG dans la banque BSG. Lorsque l'opération de l'étape 6 est effectuée, le serveur de gestion

SG informe le site marchand SM à l'étape 7 que la transaction s'est bien déroulée et que le livre L peut être expédié au client C. Le serveur de gestion SG fournit également l'adresse complète du client C au site marchand SM. Le site marchand SM expédie à l'étape 8 le livre L au client C.

Pour un nombre élevé de transactions, on peut envisager un serveur de gestion central relié à une pluralité de serveurs de gestion secondaires, chaque serveur de gestion secondaire étant lié à un opérateur de téléphonie mobile donné de façon à traiter les étapes 3 et 4.

Lorsque le client C reçoit le livre L, le serveur de gestion est informé par exemple à l'aide d'un accusé de réception envoyé par le service de livraison du livre L. Puis, à l'étape 9, le serveur de gestion SG contacte sa banque BSG afin de débiter son compte d'une certaine somme et créditer à l'étape 10 le compte du site marchand SM à la banque BSM.

Afin d'améliorer la sécurité, on peut réaliser les étapes 2 et 7 de communication entre le serveur de gestion SG et le site marchand SM à l'aide du procédé d'identification sécurisée à travers le réseau Internet. Le serveur de gestion SG et le site marchand SM possèdent alors chacun une table de données identique afin d'utiliser le procédé d'identification sécurisée. L'étape 2 peut être réalisée de la façon suivante :

- le site marchand envoie un message au serveur de gestion SG,
- en recevant le message, le serveur de gestion SG lance un défi au site marchand SM afin de vérifier l'identité dudit site marchand SM à l'aide d'un code serveur,
- le site marchand SM répond au défi en retournant un code marchand,
- le serveur de gestion SG valide le message lorsque le code marchand égale le code serveur.

L'étape 7 peut être réalisée de la façon suivante :

- le serveur de gestion SG envoie un défi au site marchand SM,
- le site marchand SM retourne un code marchand,
- le serveur de gestion SG vérifie le code marchand,

- si le code marchand est exact (code serveur égal code marchand), le serveur de gestion SG informe le site marchand SM que la transaction avec le client s'est bien passée. Le serveur de gestion SG envoie les coordonnées du client au site marchand SM ainsi que l'ordre de livraison du produit acheté par le client.

Par ailleurs, les étapes 2 et 7 peuvent être réalisées sous forme chiffrée de manière classique à travers le réseau Internet.

Finalement, on peut encore envisager un autre mode de réalisation de l'étape 2. En fait, au lieu que le numéro de téléphone du client passe d'abord par le site marchand SM pour atteindre le serveur de gestion SG, on peut relier directement le client C au serveur de gestion SG. Pour ce faire, lorsque le client choisit de payer par la transaction sécurisée, le programme informatique stocké dans le site marchand connecte, par un lien hypertexte par exemple, le client C sur un site du serveur de gestion SG. Le client C transmet alors directement ses coordonnées (numéro de téléphone mobile et pays de résidence par exemple) au serveur de gestion SG.

On voit sur la figure 2 une progression chronologique d'un mode de réalisation de l'invention. Après que le client a choisi son article, le site marchand lui demande le type de paiement. Le client désigne le type de paiement géré par le serveur de gestion SG. Ensuite le client communique son numéro de téléphone mobile au site marchand. Le site marchand transmet de manière sécurisée vers le serveur de gestion son numéro de référence, les informations concernant l'achat, ainsi que le numéro de téléphone du client. Le serveur de gestion valide l'enregistrement du site marchand et du client et appelle le téléphone mobile du client via un opérateur de télécommunication. Le serveur de gestion envoie les informations concernant l'achat selon la norme SMS, demande que le client confirme en tapant son code secret, parallèlement le serveur de gestion lance un défi. Le client valide son achat en tapant son code secret. Le serveur de gestion enregistre la confirmation qu'il communique ensuite au site marchand avec les

coordonnées du client. En même temps, le serveur de gestion vire sur con compte bancaire la somme correspondant à l'achat, ladite somme étant prélevée sur le comte bancaire du client. Il confirme le virement au client selon la norme SMS. Le site marchand envoie l'article au client. Lorsque l'article est livré au client, et après confirmation de livraison obtenue directement auprès des livreurs, le serveur de gestion contacte sa banque qui vire le montant de l'achat sur le compte bancaire du site marchand. On peut envisager que le client ait la possibilité de se connecter au serveur de gestion avec mot de passe pour consulter la liste de ses achats dans le mois ou sur une période déterminée. Du côté du site marchand, on peut envisager que le serveur de gestion gère de la même manière la liste des commandes obtenues par le site marchand.

Le procédé décrit ci-dessus permet de réaliser une transaction sécurisée sans transmission de numéro de carte de crédit à travers le réseau de communication en limitant ainsi les risques de vol. Le site marchand n'expédie l'achat du client que lorsque ledit client a payé, et le compte bancaire du site marchand n'est créditer que lorsque le client a reçu son achat. Le procédé permet de référencer aussi bien les clients que les sites marchands, et il est peu gourmand en capacité de mémoire utilisée dans la carte SIM.

Bien sûr, la présente invention n'est pas limitée aux exemples qui viennent d'être décrits. Ainsi on pourra par exemple envisager des modes de transmission de messages autres que les messages SMS. Par ailleurs, des supports d'information autres que les cartes au standard SIM pourront être mis en œuvre dans les téléphones mobiles pour contenir les tables.

REVENDICATIONS

1. Procédé de gestion d'une transaction sécurisée à travers un réseau de communication (I), par exemple de type Internet, dans lequel un client (C), lors de la commande d'un produit (L) sur un site marchand (SM), transmet (1) son numéro d'identifiant vers le site marchand à travers le réseau de communication, caractérisé en ce que :

- le site marchand transmet (2) ensuite les références du produit, l'identifiant du client et l'identifiant dudit site marchand vers un serveur de gestion (SG),
- le serveur de gestion (SG) transmet un message sur le téléphone mobile (TM) dudit client afin d'obtenir (4) l'accord du client et une authentification dudit client, puis
- le serveur de gestion (SG) confirme (7) l'accord du client au site marchand (SM) qui délivre (8) le produit commandé (L) au client (C).

2. Procédé selon la revendication précédente, caractérisé en ce que l'authentification met en œuvre une table d'identification du client (C) stockée dans un moyen de stockage du téléphone mobile dudit client ainsi que dans le serveur de gestion (SG), et en ce que le serveur de gestion possède une base de données capable de gérer une multitude de tables.

3. Procédé selon la revendication 2, caractérisé en ce que la table d'identification du client est stockée dans le moyen de stockage du téléphone mobile du client de manière codée de sorte que l'accès à ladite table d'identification par un logiciel de communication (PI) nécessite un code secret uniquement connu par le client et par le serveur de gestion (SG).

4. Procédé selon l'une des revendications 2 ou 3, caractérisé en ce que, à chaque authentification du client, le serveur de

gestion (SG) réduit la table d'identification du client stockée dans ledit serveur de gestion (SG).

5. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le serveur de gestion possède un ensemble de données sur le client, notamment des coordonnées bancaires nécessaires pour débiter (5, 6) le compte bancaire dudit client.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le serveur de gestion possède un ensemble de données sur le site marchand, notamment des coordonnées bancaires nécessaires pour alimenter (9, 10) le compte bancaire dudit site marchand une fois que le client a reçu le produit commandé.

7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la communication (2, 7) entre le serveur de gestion (SG) et le site marchand (SM) s'effectue de manière chiffrée.

8. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le numéro d'identifiant du client est un numéro du téléphone mobile (TM) du client (C).

9. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le message envoyé (3) au client par le serveur de gestion comprend les références du produit commandé, et en ce que les messages échangés (3, 4) entre le client et le serveur de gestion sont chiffrés.

10. Système de gestion d'une transaction sécurisée à travers un réseau de communication, par exemple de type Internet, comprenant :

- un site marchand (SM) connecté au réseau de communication (I),

- un point d'accès (MO) connecté au site marchand à travers le réseau de communication, le point d'accès étant utilisé par un client (C) désirant acheter un produit sur le site marchand, et
- un serveur de gestion (SG) pour :
  - recevoir (2) un identifiant du client (C) par le site marchand (SM),
  - authentifier le client en communicant (3, 4) avec ledit client à travers un téléphone mobile (TM) dudit client, l'authentification nécessitant notamment que le client tape un code secret sur son téléphone mobile,
  - débiter (5, 6) le compte bancaire du client,
  - adresser (7) une confirmation de transaction audit site marchand une fois le client authentifié et son compte bancaire débité, et
  - recevoir une confirmation de livraison du produit chez le client afin de créditer (9, 10) le compte bancaire du site marchand.

11. Système selon la revendication précédente, caractérisé en ce que le téléphone mobile du client comporte un moyen de stockage dans lequel est stocké un logiciel de communication (PI) avec le serveur de gestion.

12. Système selon l'une des revendications 10 ou 11, caractérisé en ce que le serveur de gestion est agencé pour gérer, pour chaque client, une liste des transactions effectuées sur une période donnée.

13. Système selon l'une des revendications 10 à 12, caractérisé en ce que le serveur de gestion est agencé pour gérer, pour chaque site marchand, une liste des commandes obtenues sur une période donnée.

FIGURE 1

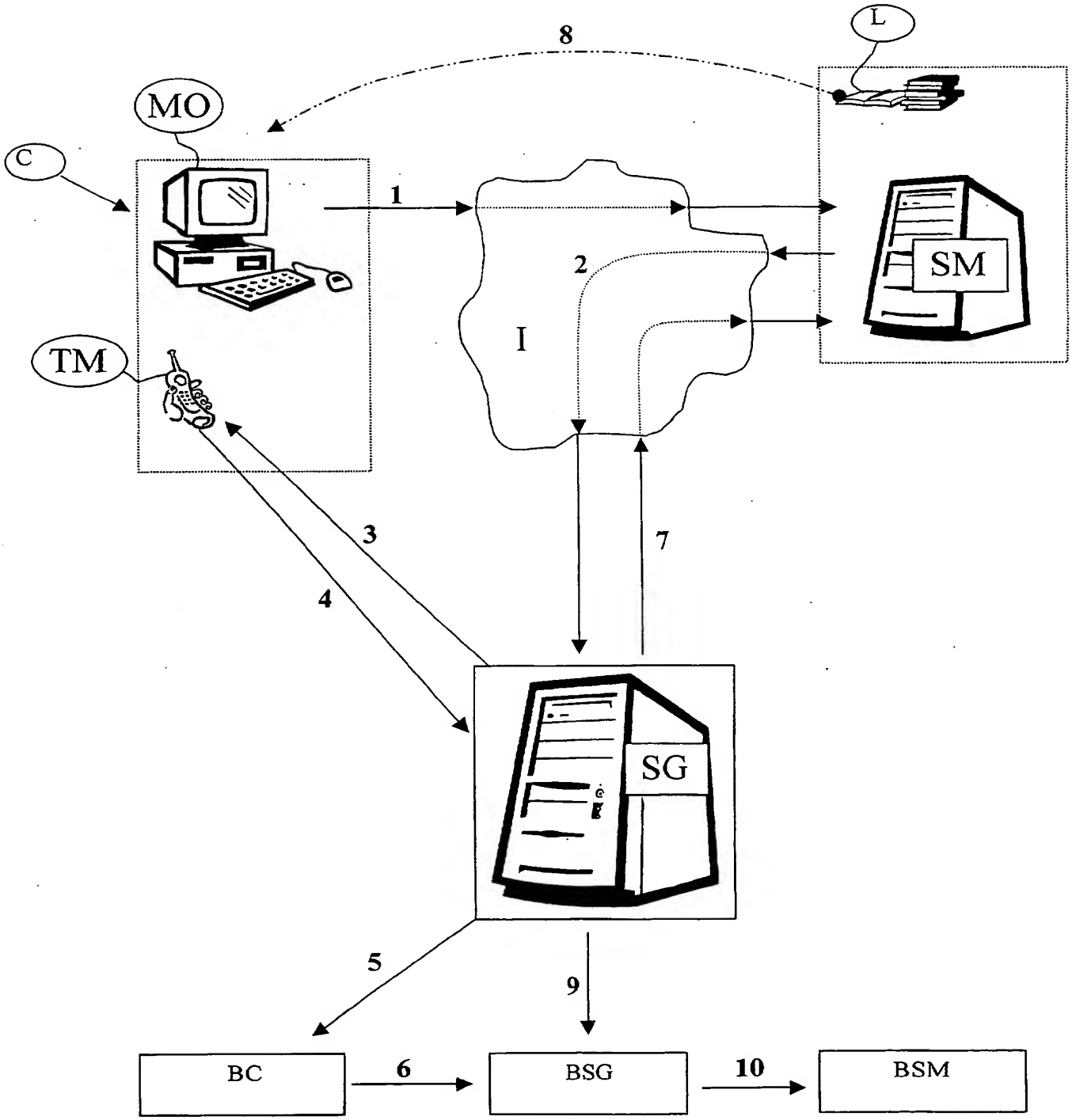
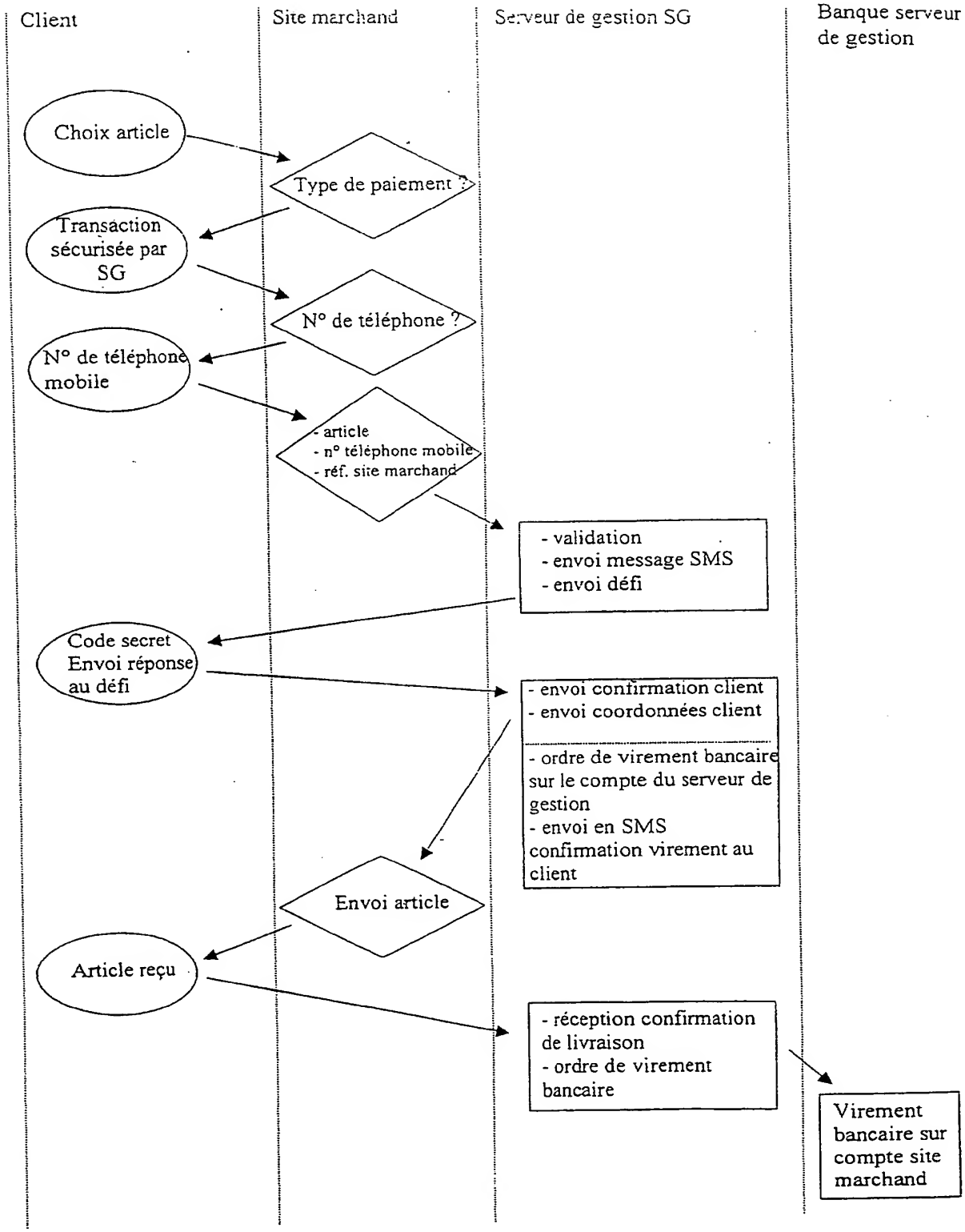


FIGURE 2


Client
Site marchand
Serveur de gestion SG
Banque serveur de gestion
Choix article
Type de paiement ?
Transaction sécurisée par SG
N° de téléphone ?
N° de téléphone mobile
- article
- n° téléphone mobile
- réf. site marchand
- validation
- envoi message SMS
- envoi défi
Code secret
Envoi réponse au défi
- envoi confirmation client
- envoi coordonnées client
- ordre de virement bancaire sur le compte du serveur de gestion
- envoi en SMS confirmation virement au client
Envoi article
Article reçu
- réception confirmation de livraison
- ordre de virement bancaire
Virement bancaire sur compte site marchand

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2801995
N° d'enregistrement national

FA 583185
FR 9915437

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
Y	WO 98 40809 A (CHA TECHNOLOGIES) 17 septembre 1998 (1998-09-17)	1,5,6,10	G06F17/60 H04L9/32
A	* abrégé; revendications; figures * * page 14, ligne 23 - page 17, ligne 26 *	2,3,7,9	H04Q7/20
Y	WO 96 00485 A (TELEFONAKTIEBOLAGET LM ERICSSON) 4 janvier 1996 (1996-01-04)	1,5,6,10	
A	* abrégé; revendications; figures *	2,3,7-9, 11	
A	US 5 986 565 A (I. ISAKA) 16 novembre 1999 (1999-11-16) * abrégé; revendications; figure 1 * * colonne 3, ligne 28 - colonne 4, ligne 46 *	1,5,6,8, 10,12	
A	WO 99 23617 A (G. KREMER) 14 mai 1999 (1999-05-14) * abrégé; revendications; figures 11-13 * * page 34, ligne 16 - page 41, ligne 19 *	1,5-10	
A	WO 96 29667 A (E. SANDBERG-DIMENT) 26 septembre 1996 (1996-09-26)		DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
A	WO 98 37524 A (SWISSCOM) 27 août 1998 (1998-08-27)		G07F

1

Date d'achèvement de la recherche	Examinateur
19 septembre 2000	David, J

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)